

Daily Threat Intelligence Briefing

Today's threat briefing contains live links that connect you to the original source articles. You can see the real URL by hovering your mouse over the links and checking that they match the source articles. These links were taken straight from the website of the source article. Tyler Technologies has not checked these sites or links for security.

News from Thursday January 22, 2026 (Reported on Friday January 23, 2026)

Government

CISA Adds Four Known Exploited Vulnerabilities to Catalog

Read more at [Cisa.gov](https://www.cisa.gov)

Financial Institutions

Securing Banking Enterprises as Non-Human Identities Grow

Read more at [BankInfoSecurity](https://www.bankinfosecurity.com)

NCUA Moves To Ease Childcare, Eldercare Burden For Volunteer Credit Union Board Members

Read more at [CUtoday.info](https://www.cuinfo.com)

Healthcare

Why HIPAA Security Risk Analyses Still Fall Short

Read more at [HealthcareInfoSecurity](https://www.healthcareinfosecurity.com)

HHS-OIG Report Highlights Key HHS Cybersecurity Challenges

Read more at [TheHIPAAJournal](https://www.hhs.gov)

Other

SmarterMail auth bypass flaw now exploited to hijack admin accounts

Read more at [Bleeping Computer](https://www.bleepingcomputer.com)

Microsoft Teams to add brand impersonation warnings to calls

Read more at [Bleeping Computer](https://www.bleepingcomputer.com)

Okta SSO accounts targeted in vishing-based data theft attacks

Read more at [Bleeping Computer](https://www.bleepingcomputer.com)

Curl ending bug bounty program after flood of AI slop reports

Read more at [Bleeping Computer](https://www.bleepingcomputer.com)

INC ransomware opsec fail allowed data recovery for 12 US orgs

Read more at [Bleeping Computer](https://www.bleepingcomputer.com)



**News from Thursday January 22, 2026
(Reported on Friday January 23, 2026)**

Why Active Directory password resets are surging in hybrid work

Read more at [Bleeping Computer](#)

Hackers exploit 29 zero-days on second day of Pwn2Own Automotive

Read more at [Bleeping Computer](#)

